Lascar群による超仮想元の特徴づけに関して (幾何学的モデル理論の研究)

AUTHOR(S):
玉江, 伸成

数理解析研究所講究録 1283 巻 2002 年 48-54

Lascar 群による超仮想元の特徴づけに関して

東京大学数理科学研究科・ 玉江 伸成 (Tamae Nobuaki)
Graduate School of Mathematical Sciences
University of Tokyo

一階の理論に関する Lascar 群は、代数学（体論）で云うところの絶対ガロア群の拡張になっている。実際、標数 0 の代数閉体の理論では両者は一致する。一方で、Lascar 群に現れるある自然な部分群が、モデル理論で以前から使われているある種の (hyper)imaginary element を特徴づけるものとなる。以下では、研究集会で行なった Lascar 群に関する速成講座を補足する形で、これらの関係を簡単な証明付で紹介していく。

1. 定義と例

以下、T で可算言語 L の完全な理論を、$\mathbf{C}$ で T の飽和モデルを表すことにする。理論によっては飽和モデルの存在が示せないこともあるが、その時は充分大きい saturation を持ったモデルを考えれば、議論はほぼ同様に進む。

定義 1.1 ある $\mathbf{C}$ の基本部分モデル (elementary submodel) を固定するような $\mathbf{C}$ の自己同型写像全体を考える。これら全てから生成される $\mathrm{Aut}(\mathbf{C})$ の部分群を $\mathrm{Autf}(\mathbf{C})$ と書き、強自己同型写像群 (strong automorphism group) と呼ぶ。$a, b \in \mathbf{C}$ がある強自己同型写像で移り合うとき、a と b の（$\mathbf{C}$ での）Lascar 強タイプが等しいと言い、$\mathrm{lstp}_{\mathbf{C}}(a) = \mathrm{lstp}_{\mathbf{C}}(b)$ と表す。

$\mathrm{Autf}(\mathbf{C})$ は $\mathrm{Aut}(\mathbf{C})$ の正規部分群となる事が容易に分かるので、$\mathrm{Aut}(\mathbf{C})/\mathrm{Autf}(\mathbf{C})$ は群となる。よって次が定義される。

定義 1.2 $\mathrm{Aut}(\mathbf{C})/\mathrm{Autf}(\mathbf{C})$ を $\mathbf{C}$ の (Lascar) ガロア群と呼び、$\mathrm{Gal}(\mathbf{C})$ と書く。

補題 1.3 M, N を $\mathbf{C}$ の基本部分モデル、$f, g \in \mathrm{Aut}(\mathbf{C})$ とする。このとき、$\mathrm{tp}(f(M)/N) = \mathrm{tp}(g(M)/N)$ ならば $f/\mathrm{Autf}(\mathbf{C}) = g/\mathrm{Autf}(\mathbf{C})$.

(証明) 仮定より $h(f(M)) = g(M)$ となるような N を固定する $h \in \mathrm{Aut}(\mathbf{C})$ がとれる。$g = h \cdot f \cdot (f^{-1}h^{-1}g)$ において、h は N を、$f^{-1}h^{-1}g$ は M を固定するので、それぞれ $\mathrm{Autf}(\mathbf{C})$ の元となる。よって $f/\mathrm{Autf}(\mathbf{C}) = g/\mathrm{Autf}(\mathbf{C})$.
(証明終)

$\mathbf{C}'$ を別の飽和モデルとする。次の定理はガロア群が飽和モデルの取り方によらないことを示す。

定理 1.4　$\mathrm{Gal}(\mathbf{C}) = \mathrm{Gal}(\mathbf{C}')$
(証明)　$\mathbf{C} \prec \mathbf{C}'$ かつ $|\mathbf{C}| < |\mathbf{C}'|$ として示せばよい。$f \in \mathrm{Aut}(\mathbf{C})$ に対し、f を拡大して得られる $\mathbf{C}'$ の自己同型 f' を任意にひとつとる。他の $f \subset f'_0 \in \mathrm{Aut}(\mathbf{C}')$ を取ったとき、$f'_0 f'^{-1}$ は $\mathbf{C}$ を固定するので強自己同型である。よって $f \mapsto f'/\mathrm{Aut}(\mathbf{C}')$ で、$\mathrm{Aut}(\mathbf{C})$ から $\mathrm{Gal}(\mathbf{C}')$ への写像が定まる。これから誘導される $\mu : \mathrm{Gal}(\mathbf{C}) \to \mathrm{Gal}(\mathbf{C}')$ が群の同型写像であることを見る。
単射性　$\mu(f) = 1$ となるような $f \in \mathrm{Aut}(\mathbf{C})$ をとる。$\mu(f)$ の代表元 $f' \in \mathrm{Autf}(\mathbf{C}')$ をとる。$M \prec \mathbf{C}$ に対し、$\mathrm{lstp}_{\mathbf{C}'}(M) = \mathrm{lstp}_{\mathbf{C}'}(f'(M))$ だから、$\mathbf{C}'$ の saturation と $f(M) = f'(M)$ より $\mathrm{lstp}_{\mathbf{C}}(M) = \mathrm{lstp}_{\mathbf{C}}(f(M))$。よって、$f \in \mathrm{Autf}(\mathbf{C})$ となる。
全射性　$f \in \mathrm{Aut}(\mathbf{C}')$ とする。$M_0 \prec \mathbf{C}$ に対し、$\mathrm{tp}(f(M_0)/N) = \mathrm{tp}(M_1/N)$ なる $M_1 \prec \mathbf{C}$ がとれる。$\mathrm{tp}(M_0) = \mathrm{tp}(M_1)$ より、$g(M_0) = M_1$ なる $g \in \mathrm{Aut}(\mathbf{C})$ をとり、更にそれを $g' \in \mathrm{Aut}(\mathbf{C}')$ に拡大する。この時、$\mathrm{tp}(g'(M_0)/N) = \mathrm{tp}(f(M_0)/N)$ となるので、補題 1.3 より、$g'/\mathrm{Autf}(\mathbf{C}) = f/\mathrm{Autf}(\mathbf{C})$ となる。
(証明終)

ガロア群が飽和モデルの取り方によらないことが示されたので、次の定義ができる。

定義 1.5　完全な理論 T に対し、$\mathrm{Gal}(T) := \mathrm{Gal}(\mathbf{C})$ （ただし、$\mathbf{C}$ は T のある飽和モデル)。

例 1.6　(1) $T = \mathrm{ACF}_0$ のとき、複素数体 $\mathbf{C}$ は飽和モデルになっている。一方 $\overline{\mathbf{Q}}$ の元は（モデル論の言葉で）代数的なので、任意の強自己同型は $\overline{\mathbf{Q}}$ を固定する。従って、$\mathrm{Gal}(T) = \mathrm{Gal}(\mathbf{C}) = \mathrm{Aut}(\mathbf{C})/\mathrm{Aut}(\mathbf{C}/\overline{\mathbf{Q}}) = \mathrm{Aut}(\overline{\mathbf{Q}})$. よって代数で云う絶対ガロア群に等しい。

(2) 最も易しい構造として、$L = \emptyset$, $T =$（無限集合の理論）を考える。この時、$\mathrm{Gal}(T) = \{1\}$ となる。
(証明)　M を可算集合とする。任意の M の置換 f が、ある無限集合を固定した M の置換の有限回の合成で書けることを見れば良い。$a \in M$ に対し $S_a = \{f^n(a) | a \in \mathbf{Z}\}$ と置く。M を S_a の形の disjoint union で分解する：$M = \bigsqcup_{i \in I} S_{a_i}$. $|I| = \infty$ なら I を 2 つの無限集合 I_0, I_1 に分解して、$\bigsqcup_{i \in I_0} S_{a_i}$ を固定する写像と $\bigsqcup_{j \in I_0} S_{a_j}$ を固定する写像の合成を考えれば良い。

$|I| < \infty$ のときも、S_{a_i} を無限集合にする i が少なくとも 2 種類あれば、S_{a_i} を固定する写像と $M - S_{a_i}$ を固定する写像の合成で書ける。残りは S_{a_i} を無限集合にする i がただ一つの時だが、$M = S_{a_i}$ として一般性を失わない。更に M の元を f で移る順番に $\mathbf{Z}$-型に並べれば（: $M = \{a_i | i \in \mathbf{Z}, f(a_i) = a_{i+1}\}$)、$M = \mathbf{Z}$, $f(n) = n + 1$ と見なせる。ここで、

$$f_0(n) = \begin{cases} n & \text{if } n \equiv 0 \pmod 3 \\ n+1 & \text{if } n \equiv 1 \pmod 3 \\ n-1 & \text{if } n \equiv 2 \pmod 3 \end{cases}$$

$$f_1(n) = \begin{cases} n+1 & \text{if } n \equiv 0 \pmod 3 \\ n+2 & \text{if } n \equiv 1 \pmod 3 \\ n & \text{if } n \equiv 2 \pmod 3 \end{cases}$$

とおけば、$f = f_1 \circ f_0$,（$f_0, f_1 \in \mathrm{Autf}(M)$） となることは単純に確かめられる。（証明終）

注意 1.7 ガロア群は上の例のように単純なものだけではない。実は、任意のコンパクト Lie 群は、ある理論のガロア群として表されることが分かっている（Bouscaren 等の未発表の結果）。

2．位相群になること

$M, N \prec \mathbf{C}$ をこの節では固定する。I-変数の N 上のタイプ全体を $S_I(N)$ で表し、その中で解が M と $\emptyset$ 上同型となるもの全てを集めたものを $S_M(N)$ と書くことにする。$S_I(N)$ に Stone 空間としての位相を入れたとき、「M と $\emptyset$ 上同型となる」というのは（無限個の）論理式の集合で書けるので、$S_M(N)$ は $S_I(N)$ の中で閉集合となり、よって（$S_M(N)$ がコンパクトかつ Hausdorff だから）コンパクトかつ Hausdorff になることに注意する。

$\mu : \mathrm{Aut}(\mathbf{C}) \to S_M(N)$, $\nu : S_M(N) \to \mathrm{Gal}(\mathbf{C})$ をそれぞれ、$\mu(f) = f(M)/N$, $\nu(f(M)/N) = f/\mathrm{Autf}(\mathbf{C})$ で定義する（$f(M)/N$ は $\mathrm{tp}(f(M)/N)$ の省略記法）。この ν による像位相で $\mathrm{Gal}(T) = \mathrm{Gal}(\mathbf{C})$ に位相を入れる。

命題 2.1 上で導入した位相は、M, N の選び方に依存しない。

（証明） M', N' を別の $\mathbf{C}$ の基本部分モデルとする。$M \prec M'$, $N \prec N'$ として一般性を失わない。$\mu' : \mathrm{Aut}(\mathbf{C}) \to S_{M'}(N')$, $\nu' : S_{M'}(N') \to \mathrm{Gal}(\mathbf{C})$ を上と同様に定義する。$\varphi : S_{M'}(N') \to S_M(N)$ を $\varphi(f(M')/N) = f(M)/N$ で定義する。

Claim. φ は連続かつ開写像。

φ は制限写像なので連続性は Stone 空間の位相の入り方から明らか。すると、$S_{M'}(N')$ も $S_M(N)$ もコンパクトかつ Hausdorff な空間なので、連続写像は自動的に開写像となる。（*Claim* の証明終）

従って $O \subseteq \mathrm{Gal}(T)$ に対し、「$\nu^{-1}(O)$ が開集合」$\iff$「$\varphi^{-1}(\nu^{-1}(O)) = \nu'^{-1}(O)$ が開集合」となる。（証明終）

$\mathrm{Gal}(T)$ の位相は、コンパクト空間の像位相なので、次が成り立つ。

命題 2.2 $\mathrm{Gal}(T)$ はコンパクト。

以下この位相で $\mathrm{Gal}(T)$ が位相群になっていることを示したいが、簡単のため、$\mathrm{Gal}(T)$ を Hausdorff 空間として証明する。

注意 2.3 Hausdorff という条件を外すと、かなり精密な議論をせねばなら

ず面倒である。方針を簡単に述べると、この時でもStone空間の性質が利いてきて、Hausdorff空間に似た性質が成り立つことがわかる。その後の証明の筋道は以下の証明と変わらない（[3] 参照）。なお、実際Hausdorffでないガロア群は存在する事が示されている [1]。

定理 2.3　$\mathrm{Gal}(T)$ は位相群になる。

（証明）　$\mathcal{M} = \{(\mu(f), \mu(g), \mu(fg)) \mid f, g \in \mathrm{Aut}(\mathbf{C})\}, \mathcal{I} = \{(\mu(f), \mu(f^{-1})) \mid f \in \mathrm{Aut}(\mathbf{C})\}$ とおく。

Claim.　$\mathcal{M}, \mathcal{I}$ は（$S_M(N)$ の直積位相で）閉集合。

$\mathcal{M}$ についてのみ示す（$\mathcal{I}$ の方もほぼ同様）。p, q, r の解をそれぞれ M_p, M_q, M_r と置くと、$(p, q, r) \in \mathcal{M}$ という条件は次と同じ：「M と M_q の $\emptyset$ 上のタイプ、(M, M_p) と (M_q, M_r) の $\emptyset$ 上のタイプがそれぞれ同じ」。この「」は（無限個の）論理式の集合で書けるので、従って $S_M(N)^3$ の閉集合となる。（*Claim* の証明終）

$\mathrm{Gal}(T)$ における $\cdot$, $^{-1}$ のグラフは $\nu(\mathcal{M})$, $\nu(\mathcal{I})$ そのもの。最初に置いた仮定より、$\mathrm{Gal}(T)$ はコンパクトかつHausdorffな空間だから、ν は閉写像。よって $\nu(\mathcal{M})$, $\nu(\mathcal{I})$ も閉集合となる。

$^{-1}$ が連続となることを見よう。$G = \mathrm{Gal}(T)$ とおき、$F \subseteq \mathrm{Gal}(T)$ を閉集合とする。$\nu(\mathcal{I}) \cap F \times G$ は閉集合であり、その（第２成分への）射影は、空間がHausdorffかつコンパクトゆえ閉写像であるから、F^{-1} も閉集合である。

$\cdot$ の連続性もほぼ同様に示される。（証明終）

３．$\mathrm{Gal}(T)$ のある部分群と超仮想元との関係

第２節で $\mathrm{Gal}(T)$ が位相群になることが分かったので、次のような自然な部分群が考えられる。

定義 3.1　1 を $\mathrm{Gal}(T)$ の単位元とするとき、$\Gamma(T)$ で $\{1\}$ の閉包、$\mathrm{Gal}^0(T)$ で $\{1\}$ の連結成分を表す。

この２つが $\mathrm{Gal}(T)$ の正規部分群になることは容易に確かめられる。

定義 3.2　$\mathbf{C}$ の仮想元 (imaginary element) とは、空集合上定義される $\mathbf{C}^n$ 上の同値関係の同値類のことである。同値関係を $E(x, y)$、代表元を $a \in \mathbf{C}$ とするとき、仮想元を a/E のように表す。a/E の $\mathrm{Aut}(\mathbf{C})$ による軌道が有限集合の時、仮想元 a/E が代数的であるという。

補題 3.3　強自己同型写像は代数的な仮想元を動かさない。

（証明）　$\mathrm{Autf}(\mathbf{C})$ の生成元を取ってくることにより、強自己同型写像 f はある $M \prec \mathbf{C}$ を固定するとしてよい。a/E を代数的仮想元とする。$E^n(x_1 \cdots x_n) =$

$\bigwedge_{1\leq i\neq j\leq n} \neg E(x_i, x_j)$, $p(x) = \mathrm{tp}(a)$ とするとき、ある自然数 n で、

$$\bigcup_{1\leq i\leq n} p(x_i) \cup \{E^n\} \text{ は無矛盾だが、} \bigcup_{1\leq i\leq n+1} p(x_i) \cup \{E^{n+1}\} \text{ は矛盾}$$

となるものがある。コンパクト性定理より、ある $\varphi \in p$ で、$\varphi(\mathbf{C})$ と上で取れる n 個の E-同値類を交わらせることができる。M はモデルなので、この n 個の同値類は $\varphi(M)$ とも交わっている。従って $a/E \ni b(\in M)$ なる b があるが、f は M を固定するので、$f(a/E) = a/E$ でなければならない。(証明終)

定義 3.4　$\mathbf{C}$ の超仮想元 (hyperimaginary element) とは、空集合上 type-definable な((無限個の) 論理式の集合で定義される) 同値関係の同値類のことをいう。ここで、その同値関係を $E(x, y)$ で表すとき、x の長さは無限でも構わない。a/E の $\mathrm{Aut}(\mathbf{C})$ による軌道の濃度が $|\mathbf{C}|$ のとき、超仮想元 a/E を有界 (bounded) であるという。

補題 3.5　強自己同型写像は有界な超仮想元を動かさない。

(証明)　a/E を有界な超仮想元、f を $M \prec \mathbf{C}$ を固定する $\mathbf{C}$ の自己同型、$b = f(a)$ とする。$p(x) = \mathrm{tp}(a/M)$ とおき、$p(x)$ の $M \cup \{a, b\}$ 上への非分岐拡大 (nonforking extension) の $\mathbf{C}$ での解を c_1、$M \cup \{a, b, c_1\}$ 上への非分岐拡大の $\mathbf{C}$ での解を c_2 と帰納的に $\langle c_i; i < |\mathbf{C}|\rangle$ をとると、$\langle a, c_1, c_2, \ldots\rangle$, $\langle b, c_1, c_2, \ldots\rangle$ はそれぞれ M 上の一様列 (indiscernible sequence) になっている。

ここで、$\mathbf{C} \models \neg E(a, b)$ と仮定する。$\mathbf{C} \models \neg E(a, c_1)$ とすると、全ての $i \neq j < \kappa$ で $\neg E(c_i, c_j)$ が成立するし、$\mathbf{C} \models E(a, c_1)$ とすると、$\mathbf{C} \models \neg E(b, c_1)$ が言えてしまうので、再び全ての $i \neq j < \kappa$ で $\neg E(c_i, c_j)$ が成立する。いずれの場合も a/E の有界性に反するので、$\mathbf{C} \models E(a, b)$ でなければならない。従って $f(a/E) = a/E$ となり、よって題意が示される。(証明終)

実は、ある意味で補題 3.5 の逆も言える。

補題 3.6　強自己同型写像で動かない超仮想元は有界である。

(証明)　a/E を超仮想元とする。$\mathcal{E} = \{f(a)/E \mid f \in \mathrm{Aut}(\mathbf{C})\}$ を考えるが、a/E が強自己同型で動かないので、これは $\{f(a)/E \mid f/\mathrm{Autf}(\mathbf{C}) \in \mathrm{Gal}(\mathbf{C})\}$ と同じ集合である。第2節の M, N を濃度 $|T|^+$ のモデルにとると $|\mathrm{Gal}(\mathbf{C})\}| \leq |S_M(N)| \leq 2^{|T|^+}$ となり、従って $|\mathcal{E}| \leq 2^{|T|^+}$ となる。よって a/E は有界である。(証明終)

とすると、全ての有界な超仮想元を動かさない自己同型は強自己同型であるようにも思われるが、実はそうではない。正確には、3.1 で定義した $\Gamma(T)$ がそのような自己同型に対応している。すなわち、

定理 3.7　$\Gamma(T) = \{f/\mathrm{Autf}(\mathbf{C}) \in \mathrm{Gal}(\mathbf{C}) \mid f$ は任意の有界な超仮想元を固

（証明） 有界な超仮想元 a/E に対し、$\mathrm{Stab}(a/E)$ を a/E を固定する $\mathrm{Gal}(\mathbf{C})$ の元全ての集合とする。$a \in M, N \prec \mathbf{C}$ となるように M, N を選ぶと、

$$\begin{aligned}\nu^{-1}(\mathrm{Stab}(a/E)) &= \{\mathrm{tp}(f(M)/N) \mid f \in \mathrm{Aut}(\mathbf{C}), \mathbf{C} \models E(f(a), a)\} \\ &= \{p(x) \in S_M(N) \mid E(x_0, a) \subset p(x)\}\end{aligned}$$

（$x_0 \subset x$ は $a \in M$ に対応する変数） となり、従って $S_M(N)$ の位相で閉集合となることが分かる。従って $\mathrm{Stab}(a/E)$ も閉集合となる。$\Gamma(T)$ は $\{1\}$ を含む最小の閉集合だから、$\Gamma(T) \subseteq \mathrm{Stab}(a/E)$. 従って $\Gamma(T) \subseteq \bigcap_{a/E:\text{有界}} \mathrm{Stab}(a/E)$ となる。これは定理のステートメントの（$\subseteq$）を意味する。

逆（$\supseteq$）を示す。$G/\mathrm{Autf}(\mathbf{C}) = \Gamma(T)$ となるように $G \leq \mathrm{Aut}(\mathbf{C})$ をとる。M で番号づけられている2つの列 a, b に対して、同値関係 E を、$E(a,b) \overset{\text{def}}{\Longleftrightarrow}$ 「a, b は同じ G-軌道に入っている」で定義する。E が $\emptyset$ 上 type-definable で有界な同値関係であることが示されれば充分である。

まず、$|\mathrm{Aut}(\mathbf{C})/G| \leq |\mathrm{Gal}(T)/\Gamma(T)| \leq |\mathrm{Gal}(T)|$ より、G-軌道、すなわち E-同値類の個数は $|\mathrm{Gal}(T)|$ 以下なので、有界である。

次に $\Gamma(T)$ は閉集合なので、$\nu^{-1}(\Gamma(T)) = \{p(x) \in S_M(N) \mid p_0(x) \subseteq p(x)\}$ となる論理式の集合 $p_0(x)$ がある。

$$\begin{aligned}E(a,b) &\iff \exists f \in \mathrm{Aut}(\mathbf{C})\ \ \mathbf{C} \models f(a) = b \wedge p_0(f(M)) \\ &\iff \exists x\ \text{“}\mathrm{tp}(aM) = \mathrm{tp}(bx)\text{''} \cup p_0(x)\end{aligned}$$

となるので、これは（無限個の）論理式の集合で書ける条件である。更に G は $\mathrm{Aut}(\mathbf{C})$ の正規部分群だから、E は自己同型で不変である。従って $\emptyset$ 上の論理式の集合で書けている。（証明終）

代数的な仮想元に対しても、定理 3.7 に類した特徴づけがある。

定理 3.8 $\mathrm{Gal}^{\circ}(T) = \{f/\mathrm{Autf}(\mathbf{C}) \in \mathrm{Gal}(\mathbf{C}) \mid f$ は任意の代数的な仮想元を固定する $\}$

証明には profinite group で知られた事実を使って、定理 3.7 に似た論法を用いるが、やや複雑である。詳細は [3] を参照。

それぞれの理論 T に対し、$\mathrm{Gal}^{\circ}(T)$ や $\Gamma(T)$ が単位元からなる群と一致するかは、（超）仮想元の性質を調べる上で重要である。例えば、T が安定な理論とする。$\mathrm{tp}(a/\mathrm{acl}^{eq}(\emptyset)) = \mathrm{tp}(b/\mathrm{acl}^{eq}(\emptyset))$ なら、ab と（$\emptyset$ 上）独立な任意のモデル M に対し、$\mathrm{tp}(a/M) = \mathrm{tp}(b/M)$ となるので、代数的な仮想元を動かさない自己同型はあるモデルを固定できる。よって定理 3.8 より、$\mathrm{Gal}^{\circ}(T) = \{1\}$ となる。他にも、T が単純な理論のときは、$\Gamma(T) = \{1\}$ であることは示されているが [2]、$\mathrm{Gal}^{\circ}(T) = 1$ であるかどうかは未解決の問題となっている。

参考文献

[1] Casanovas, E.; Lascar, D.; Pillay, A.; Ziegler, M. Galois groups of first order theories. *J. Math. Log.* 1 (2001), no.2, 305–319.

[2] Kim, Byunghan. A note on lascar strong types in simple theories. *J. Symbolic Logic*, 63 (1998), no.3, 926-936

[3] Ziegler, M. Introduction to the Lascar group. Preprint, 2001